[19] 中华人民共和国国家知识产权局

[51] Int. Cl⁷
G11B 20/00
G06F 1/00

[12] 发明专利申请公开说明书

[21] 申请号 01803152.8

[43] 公开日 2003 年 1 月 22 日

[11] 公开号 CN 1393017A

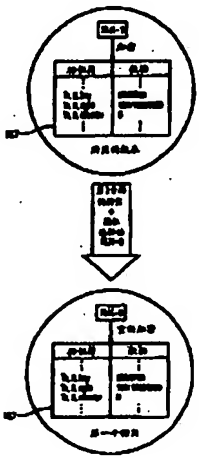
[22] 申请日 2001.8.2 [21] 申请号 01803152.8
[30] 优先权
[32] 2000.8.16 [33] EP [31] 00202888.4
[86] 国际申请 PCT/EP01/08924 2001.8.2
[87] 国际公布 WO02/15184 英 2002.2.21
[85] 进入国家阶段日期 2002.6.14
[71] 申请人 皇家菲利浦电子有限公司
地址 荷兰艾恩德霍芬
[72] 发明人 M·A·特雷菲尔斯
A·A·M·斯塔林
[74] 专利代理机构 中国专利代理(香港)有限公司
代理人 吴立明 陈 霁

权利要求书 2 页 说明书 9 页 附图 3 页

[54] 发明名称 用于控制数字作品的发行和使用的方法和装置

[57] 摘要

本发明涉及一种用于控制与附加的使用权信息一起存储在记录载体上的数字作品的发行和使用的方法和装置。该附加的使用权信息被用一个在使用权信息每次改变时就改变的隐蔽信息加密或验证。该使用权信息可以是一个用于加密使用权信息的加密密钥，或者是含有该使用权信息的一个数据块的校验和。这样，“复制并恢复侵袭”就不能成功，因为这将导致该隐蔽信息与所恢复的使用权信息的不匹配。



ISSN1008-4274

1.一种用于控制数字作品（DW）的发行和使用的方法，包含下述步骤:

a) 将一个使用权信息附加到所述数字作品(DW)，所述使用权信息定义一个或多个为了行使所述使用权而必须满足的条件;

b)在记录载体(10)上存储所述数字作品(DW)及其附加的使用权信息;

c)随着所述数字作品(DW)的每一次使用而更新所述附加的使用权信息;

d)如果所述使用权信息表明该使用权已经被行使，则拒绝所述数字作品的使用;

特征在于:

e)当使用权信息已经改变时，存储在一个隐蔽信道中的用于加密和验证所述使用权信息的隐蔽信息被改变。

2.按照权利要求 1 的方法，特征在于，所述隐蔽信息是含有所述使用权信息的数据块上的一个校验和。

3..按照权利要求 1 的方法，特征在于，所述隐蔽信息是一个用于解密所述使用权信息的密钥(KLK)，其中，当所述使用权信息变化时，所述密钥被随机地改变，并且所述使用权信息被通过使用所述改变的密钥重新加密。

4 .按照权利要求 3 的方法，特征在于，在先的密钥(KLK-1)在所述密钥的改变之后被销毁。

5 .按照权利要求 1 至 3 的任何一项的方法，特征在于，所述隐蔽信道被安排成是商业复制装置不能访问的。

6 .按照权利要求 5 的方法，特征在于，所述隐蔽信道是以下述方式生成的:

-在能被再更正的故意错误中存储所述隐蔽信息(KLK);

-在一个运行长度限制码的合并位中存储所述隐蔽信息(KLK);

-按照 所述隐蔽信息(KLK)，控制一个运行长度限制码的预定字的预定游程的极性;

-在时间基中的故意错误中存储所述隐蔽信息(KLK); 或者

-在内置在盘控制器的存储器中存储所述隐蔽信息(KLK)。

7.按照权利要求 2 至 6 的任何一项的方法，特征在于，所述附加的使用权信息与一个被用于解密所述数字作品(DW)的密钥信息一起存储在一个表(KLT)中。

8. 按照权利要求 1 至 7 的任何一项的方法，特征在于，所述数字作品(DW)是一个从因特网下载的声道，所述记录载体是可记录光盘、硬盘、磁-光记录装置、磁带或存储器卡。

9.按照权利要求 1 至 8 的任何一项的方法，特征在于，所述使用权信息包含一个在所述使用权已经被行使时能被更新的计数器信息。

10 .按照权利要求 1 至 9 的任何一项的方法，特征在于，记录介质的每个道包含其自己的使用权信息和隐蔽信息(KLK)。

11 一种存储数字作品（DW）和定义一个或多个为了行使使用权而必须满足的条件的使用权信息的记录载体，特征在于，所述记录载体(10)包含一个是商业复制装置不能访问的隐蔽信道，在该隐蔽信道中存储一个隐蔽信息，该隐蔽信息被用于加密或验证所述使用权信息，并且在所述使用权信息改变时而被改变。

12.按照权利要求 11 的记录载体，特征在于，所述记录载体是可记录光盘(10)，特别是 CD 或 DVD。

13. 一种用于控制数字作品的发行和使用的装置，包含:

a)写装置(20)，用于在一个记录载体(10)上写所述数字作品和附加的、定义一个或多个为了行使使用权而必须满足的条件的使用权信息;

b)更新装置(22)，用于随着所述数字作品的每一次使用而更新所述附加的使用权信息; 和

c)控制装置(21)，用于在如果所述使用权信息表明该使用权已经被行使时拒绝所述数字作品(DW)的使用，

特征在于:

d)所述更新装置(22)被安排得在所述使用权信息已经改变时，改变在一个隐蔽信道中存储的用于加密和验证所述使用权信息的隐蔽信息(KLK)。

用于控制数字作品的发行和使用的方法和装置

本发明涉及用于控制数字作品的发行和使用的方法和装置。此外，本发明也涉及用于存储数字作品的记录载体。

出版业和信息产业在考虑电子出版时面临的一个根本问题是如何阻止对电子出版物的非授权和未说明的发行和使用。电子出版物一般是以数字形式发行的，并在有再现电子出版物的功能的基于计算机的系统上创建的。音像录制品、软件、书籍和多媒体作品都在被用电子方式出版。对每个有说明的传输都要支付使用费，任何未说明的发行结果是不支付使用费。

数字作品在诸如广泛使用的因特网等网络上的传送如今是常见的做法。因特网是一种分布广泛的网络，许多大学、公司、和政府部门的用户用因特网传送和交换思想和信息。所以，需要在不担心广泛的非授权复制的情况下利用这种网络来发行数字作品。

消费电器与计算机之间的显然转化、 网络和调制解调器速度的增加、计算机功能和带宽的成本的下降、以及光学介质的功能的提高，综合起来将创建极大的混合商业模式，在这些模式中，所有种类的数字内容都可以在至少偶尔相连的消费电器和/或计算机上播放的光学介质上传播，在这些模式中，增加了在音乐 CD 和初始 DVD（数字视盘）电影提供中常见的一次性购买模式以外的其它模式，例如租借、付费收视(pay-per-view)、租转获有(rent to own)。消费者可以从相同的和/或不同的分销商和/或供应商得到在这些和其它的模式中选择的许诺。使用费可以在网络上和/或通过其它通信渠道向某个费用结算业务机构支付。消费者使用和预订信息可以流回到生产者、分销商和/或其他参与者。现今正在引入的可记录光盘的基本复制保护技术不能支持这些和其它的复杂模式。

文献 US-A5629980 披露了一种用于控制数字作品的分发和使用的方法和装置，如权利要求 1 和 3 的前序中所定义的那样，其中数字或使用权是与购买一起获得的。这种使用权限制了如何能使用在因特网上购买的、下载的或者可记录光盘上的加扰形式的音乐道(music

track)。这些数字权也叫使用规则或使用权。例如，可以允许购买人为个人用途复制三份拷贝，不允许复制第四份拷贝。或者，可以允许购买者将特定的道播放四次，而光盘驱动器将不播放第 5 次。

最好将使用权存储在光盘上。在这种情况下，使用权与音乐一起转移，光盘将在所有支持这个功能的播放器上播放。

用于从因特网下载音乐道的电子音乐下载（EMD）应用程序必须在盘上存储若干信息片断，例如加扰的声道（audio track)、解扰该声道所需的密钥、以及使用权说明。有些使用权在使用时可能会被减少（即被消费）。规则“个人用途的三份拷贝”例如在已经复制了一份拷贝后变成“个人用途的两份拷贝”。使用权因此含有一个能在使用权已经被行使时被更新的计数器。

任何被安排得能访问下载的道的设备都应当顺从所购买的使用权的基本规则。就是说，只有被授权的、受委托的回放设备才能读取密钥，设置使用权或计数器。因此，应当阻止非顺从应用不更新计数器就复制音乐道，不支付额外的费用就递增计数器，或复制完全相同的具有相同使用权的复制盘。

针对采用标准盘驱动器进行的按位复制操作，已经有单位盘标识符(UDI-Unit Disk Identifier)的建议，它可以由制造商以可被回放设备读取的方式写在盘上。如果某可记录盘有 UDI，就可以将该标识符与音乐道的加扰密钥组合起来。将有关盘按位复制到另一个记录载体后，就不再能被解扰，因为该其它记录载体将有一个不同的 UDI，使得加扰密钥不能再被恢复。

然而，“复制并恢复侵袭”(copy and restore attack)或“重放侵袭”(replay attack)可以被用来克服上述 UDI 解决方案。再这种情况下，用一个标准盘来确定盘上那些在使用权被消费时已经被改变的位。这些位一般与使用权的计数器有关，因此被复制到另一个存储介质。然后，例如通过进行复制而消费使用权，直到复制计数器达到零，就不再允许进一步的拷贝。将所确定的和存储的位从该存储介质恢复到盘上。现在，该盘处于的状态，假装使用权还没有被消费或行使，使得用户可以继续进行复制。在这种情况中，依赖 UDI 的加扰密钥对复制操作没有影响，因为该盘没有被改变。

此外，文献 WO-A-97/43761 披露了一种用于诸如光学数字视盘的

存储介质的权利管理安排，其中用一个安全的“软件容器”来保护性地封装一个数字作品和对应的使用权信息。此外，还在盘上存储一个加密的密钥块，它提供一个或多个密钥用于解密该数字作品。用于解密密钥块的解密密钥，也以隐蔽的形式长存储在记录载体上，存储的位置，可以被盘驱动器的对应的固件或跳线(jumper)物理地使能。这样，任何又个人电脑物理地复制该盘的企图，结果都不能复制该隐蔽的密钥。

然而， 即使这个加密保护方法可能也不能防止“复制并恢复侵袭”，因为潜在的黑客把所检测到和复制的使用权数据恢复回它们在相同盘上原来的位置。然后，黑客可以再次播放使用权已经被行使过的道，而无须再付费。注意到黑客不必读或写隐蔽的密钥就能破解该保护机制。因此，“复制并恢复侵袭”适用于被消费了的权利，诸如播放一次的权利，制作有限数量的拷贝的权利（盘上的计数器在每次拷贝之后递增），或者将道从一个盘转移到另一个（原始盘上的道被删除）的权利。

因此，本发明的一个目的是提供一种用于根据附属的使用权和对应的记录载体控制数字作品的分发和使用的方法和装置，由此能防止使用权被“复制并恢复侵袭”破解。

该目的是通过权利要求 1 所定义的方法、权利要求 11 所定义的记录载体和权利要求 13 所定义的装置取得的。

相应地，在使用权信息已经改变时，重写使用权信息并存储用于加密和验证该使用权信息的新的隐蔽信息。这样，在“复制并恢复侵袭”过程中对使用权信息的简单恢复操作只能恢复以前的使用权信息，但是不恢复以前的隐蔽信息。然而，由于事实上改变了的隐蔽信息不再适合或对应于以前的或原始的使用权信息，对使用权信息的解密或验证不再可能，使得盘播放器的保护系统将识别欺诈的企图。对隐蔽信道的“复制并恢复侵袭”将不再有效，因为非顺从装置是不能在隐蔽的信道上读写的。

按照一个有益的进展，隐蔽信息可以是含有使用权信息的数据块上的一个校验和。在这种情况中，使用权信息不必被在记录载体上加密。通过计算校验和并把这个校验和存储在隐蔽信道中，就能防止对使用权信息的内容的任何操作。“复制和恢复”攻击不起作用，因为

已经随着使用权信息的更新而改变了的隐蔽校验和，对于恢复后的原始使用权信息来说不再有效。

或者，按照另一个有益的进展，隐蔽信息可以是一个用于解密使用权信息的密钥，其中该密钥是随机改变的，当使用权信息已经改变时，使用权信息被用改变过的密钥重新加密。恢复老版本的使用权信息将不再有用，因为改变过的密钥不能被用来解密原始的使用权信息。

最好在密钥的改变之后销毁以前的密钥。由此，用于加密原始使用权信息的密钥就不再能被提取，潜在的黑客就不能解密原始使用权信息。

隐蔽信道最好可以按下述方式生成:

在能被再更正的故意错误中存储隐蔽信息;

在运行长度限制码(runlength-limited code)的合并位中存储隐蔽信息;

按照隐蔽信息，控制一个运行长度限制码的预定字的预定游程的极性(polarity);

在时间基(time-base)中的故意错误中存储隐蔽信息; 或者

在内置在盘控制器的存储器中存储隐蔽信息。由此，就能提供一个不能被现有或常规盘驱动器读或写的隐蔽信道。即使通过固件更新，它们也不能读或写隐蔽信道。特别地，要复制或读取隐蔽信道，就要修改相应的集成电路。不过这是昂贵的，需要对应的专门知识。已知的记录载体的导入区(lead-in areas)不足以提供这样一个隐蔽信道，因为常规的盘驱动器允许通过简单的固件篡改(hacking)操作来访问这些区。

按照另一个有益的修改，可以将附属的使用权信息与用于解密数字作品的密钥信息一起存储在一个表中。这样，解密数字作品所需的密钥信息在“复制并恢复便装”之后就不再能被解密。数字作品可以是一个从因特网下载到可记录光盘的声道。

使用权信息最好包含一个能在使用权已经被行使时更新的计数器。这样，计数器信息的改变导致用新的隐蔽密钥的重写和重新加密操作，使得对更新的计数器值的探测和恢复因改变的隐蔽解密密钥而毫无用处。

按照另一个有益的修改，记录介质的每个道(track)都可以包含其

使用权信息和隐蔽信息。在这种情况中，为记录载体的每个道提供一个隐蔽密钥，只要隐蔽信道有足够的容量。

以下将结合各附图根据最佳实施例更详细地说明本发明。

图 1 表示按照本发明最佳实施例在一个复制操作之后密钥-锁表和隐蔽密钥的修改；

图 2 表示按照本发明最佳实施例的用于驱动记录载体的驱动装置的基本框图；

图 3 表示按照本发明最佳实施例的使用权信息的安全更新的基本流程图。

现在将根据一个从因特网到诸如可记录光盘的记录载体的 EMD 来说明最佳实施例，其中道是购买的、下载的或记录载体上存储的。

不过，在本申请中，术语“数字作品”指的是任何已经被缩减成一个数字表示的作品。这包括任何音频、视频、正文或多媒体作品和再现该作品所需的任何附随的解释器(例如软件)。术语“使用权”指的是向数字作品的接受者赋予的任何权利。一般来说，这些权利定义如何使用一个数字作品以及是否该数字作品可被进一步传播。每个使用权可以有为行使该权利而必须满足的一个或多个确定条件。使用权被永久地“附属”到数字作品上。从数字作品产生的拷贝也有使用权附属着。这样，使用权和由创建者和后继的发行者指派的任何相关费用将总是与数字作品保持在一起。

按照最佳实施例，所有秘密，例如使用权、密钥、计数器、盘的自我标识或任何要以防篡改的方式存储的信息，都一起存储在一个表中，该表称作密钥-锁表 KLT。 密钥-锁表 KLT 被例如用 DES 算法加密，存储在盘上任何方便的位置。用于加密密钥-锁表 KLT 的密钥叫密钥-锁密钥 KLK。密钥 KLK 被存储在盘上一个特殊的隐蔽信道或者安全侧信道中，不能被现有的或常规的盘驱动器读或写。特别地，必须将隐蔽信道安排得使得现有的盘驱动器的固件更新不足以能进行对隐蔽信道的读、写操作。

隐蔽信道必须在所记录数据流、记录载体或盘驱动器的物理特征中隐藏得非常深，以至要修改集成电路才能用现有的盘驱动器读或写隐蔽信道。实现这样一个隐蔽信道的一些可能是：

(i)在数据流的有能被再更正的故意错误中存储隐蔽信息；

KLT。特别地，一个可在计算机系统上运行以提供对应的下载功能的 EMD 应用程序，将所购买的加扰数字作品与解扰该数字作品所需的密钥以及使用权的说明一起存储在盘驱动器的存储器 23 中。或者，可以将所购买的信息片段存储在计算机系统的存储器中，盘驱动器的驱动控制器 21 可以从存储器读取这些信息。

驱动控制器 21 从存储器 23 读取所购买的信息片段，并把密钥和使用权提供给密钥-缩更新和加密单元 22，该单元被安排得能生成一个对应得密钥-锁表 KLT 并随机地控制读写(RW)单元 20 在可记录盘上的预定位置写所购买的数字作品 DW(即道)和密钥-锁表 KLT。此外，驱动控制器 21 控制 RW 单元 20 在可记录盘 10 的、常规的盘驱动器或盘播放器是不能访问的隐蔽信道中存储密钥-锁密钥 KLK。随着所购买使用权因消费（例如复制或播放操作）而发生的每一次改变，驱动控制器 21 将一个对应的控制信号提供给密钥-锁更新和加密单元 22，后者相应地更新密钥-锁表 KLT，生成一个新的随机选择的密钥-锁密钥 KLK，并用该密钥-锁密钥 KLK 加密密钥-锁表 KLT。驱动控制器 21 接收所更新和加扰的密钥-锁表 KLT 和新的密钥-锁密钥 KLK，控制 RW 单元 20 把重新加扰的密钥-锁表 KLT 写到可记录盘 10 上，把新的密钥-锁密钥 KLK 写入隐蔽信道中。就这样在密钥-锁表 KLT 内每次变化之后用一个新的密钥-锁密钥 KLK 进行更新和加密。

如果所更新的密钥-锁表 KLT 表明使用权已经被行使或消费，盘控制器 21 就例如通过向 EMD 应用程序传送一个对应的出错消息或控制信号而拒绝对相应的盘的使用。

应当注意到，密钥-锁更新和加密单元 22 可以以驱动控制器 21 的一个软件例程的形式实现。

图 3 表示以上的使用权的安全更新的过程的基本流程图。按照图 3，在可记录盘已经被装载到盘驱动器并且对应的数字作品的使用操作已经开始之后的步骤 S100，生成一个新的随机密钥-锁密钥 KLK-2。然后，由密钥-锁更新和加密单元 22 用该新的密钥-锁密钥 KLK-2 来更新的密钥-锁表 KLT 的内容(步骤 S101)。然后，该新的密钥-锁密钥 KLK-2 被 RW 单元 20 写入可记录盘 10 的隐蔽信道 HC（步骤 S102）。该步骤之后可以接着验证该新的密钥-锁密钥 KLK-2 和重新加密的密钥-锁表 KLT 已经被正确地写在可记录盘 10 上的可选步骤。最后，可以由 RW

单元销毁前一个密钥-锁密钥 KLK-1(步骤 S103)。

按照最佳实施例的一个替代性修改，密钥-锁更新和加密单元 22 可以被一个密钥锁更新和验证单元替代，该密钥锁更新和验证单元被安排得对密钥-锁表 KLT 的内容计算一个校验和并把该校验和存储在隐蔽信道 HC 中（而不是密钥-锁密钥 KLK 中）。在这种情况下，甚至不需要对密钥-锁密钥 KLK 加密。对密钥-锁表 KLT 的内容的任何操作都能被该密钥锁更新和验证单元通过使用该隐藏的校验和进行校验操作而验证。因对所购买的使用权的消费或行使而引起的密钥-锁表 KLT 的任何变化，导致一个变化的校验，变化的校验和被写入隐蔽信道 HC。这样，“复制并恢复侵袭”将导致在所恢复的密钥-锁表 KLT 的实际校验和与隐藏的校验和之间的不匹配。这个不匹配将被密钥-锁更新和验证单元检测到，使得能启动一个出错处理或保护机制。

所以，本发明具有的优点是，“复制并恢复侵袭”导致在隐藏的密钥-锁密钥 KLK 或替代性的隐藏校验和与所恢复的密钥-锁表 KLT 之间的不匹配。这种不匹配或者阻止对密钥-锁表 KLT 的解扰，或者导致验证处理中的出错。这样就能在盘驱动器中检测到欺诈性的攻击。

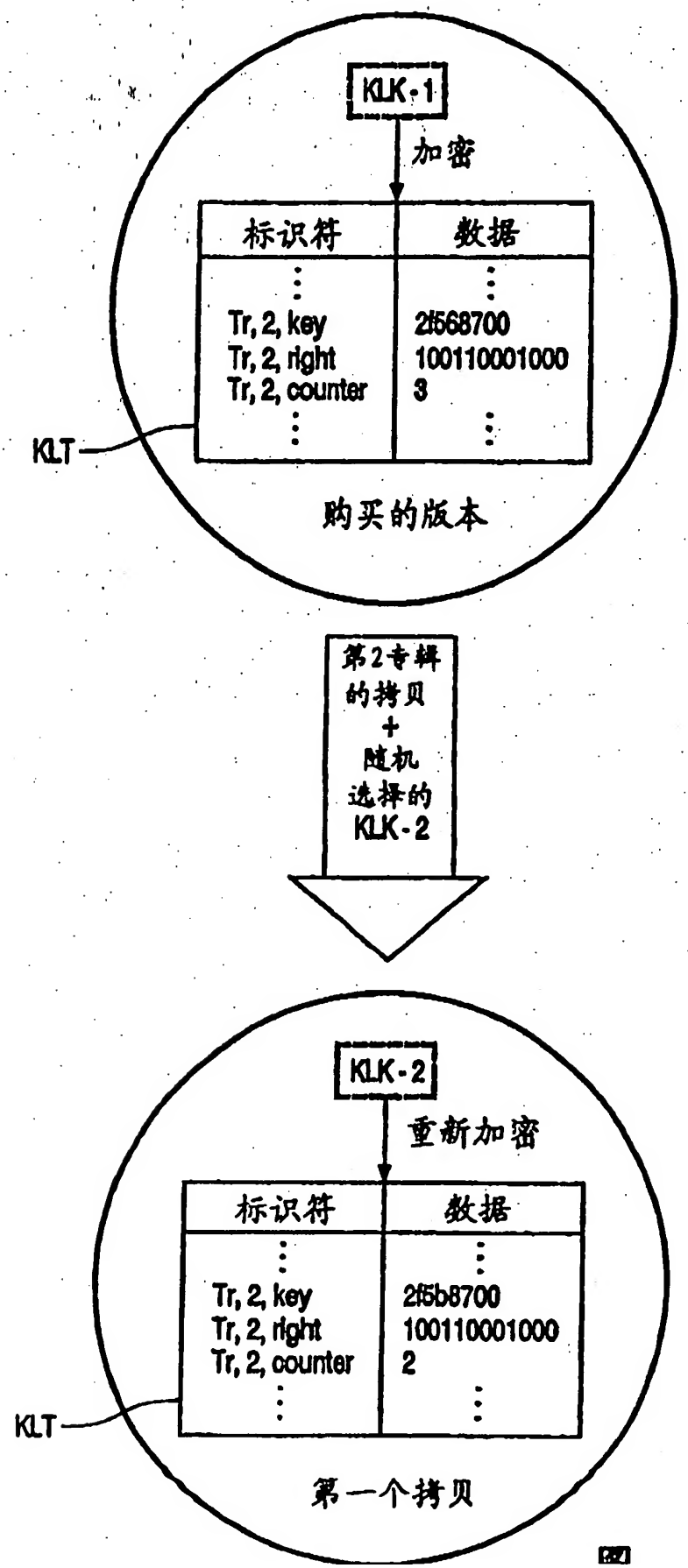
在另一个实施例中，隐蔽信道包含被用于对密钥-锁表 KLT 的内容计算一个校验和的随机数据，该校验和被存储在用户数据中，因此对于顺从装置和非顺从装置来说都是可以自由访问的。如果确定隐蔽信道的内容不能被非顺从装置确定性地改变，隐蔽信道的内容就是可以自由访问的。顺从装置可以通过读取隐蔽信道中的随机数据而计算校验和并检查所计算的校验和是否对应于存在于用户数据中的校验和。所计算的校验与存在于用户数据中的校验和的不同，表明隐蔽信道的内容可能被窜改。

注意到本发明并不限于上述实施例，而是可以应用任何应当得到防止“复制并恢复侵袭”的保护的记录或写应用。EMD 可以通过在受压盘上加扰数字作品 DW 的免费发行或者通过广播信道而执行。然而密钥则不与数字作品的内容一起发行。密钥可以通过因特网购买。在这样的情况下，不需要下载压缩的数字作品，而只要下载密钥。由此就能降低网络负荷和传输成本。

此外，可以把密钥-锁表 KLT 安排得每个道一个密钥-锁。在这种情况中，需要隐蔽信道有足够得空间能为每个密钥-锁表 KLT 存储一个

随机的密钥-锁密钥 KLK。如果密钥-锁表 KLT 变得很大，以至不能在每个交易执行一个重写操作，则可以将其分解为多个密钥-锁表。然后，每个密钥-锁表 KLT 将有其自己的、存储在隐蔽信道中的随机密钥-锁密钥 KLK。

本发明也可以应用于保护硬盘不受“复制并恢复便装”。在这种情况中， 可以把隐蔽信道安排为内置于 HDD 控制器的存储器。对闪存卡之类的类似应用也是可能的。总之，本发明可以应用于保护任何另外的记录介质，例如磁-光记录介质（小型磁盘）（minidisc)或磁带。


KLK-1
加密
标识符
数据
Tr, 2, key
Tr, 2, right
Tr, 2, counter
2f568700
100110001000
3
KLT
购买的版本
第2专辑
的拷贝
+
随机
选择的
KLK-2
KLK-2
重新加密
标识符
数据
Tr, 2, key
Tr, 2, right
Tr, 2, counter
2f5b8700
100110001000
2
KLT
第一个拷贝

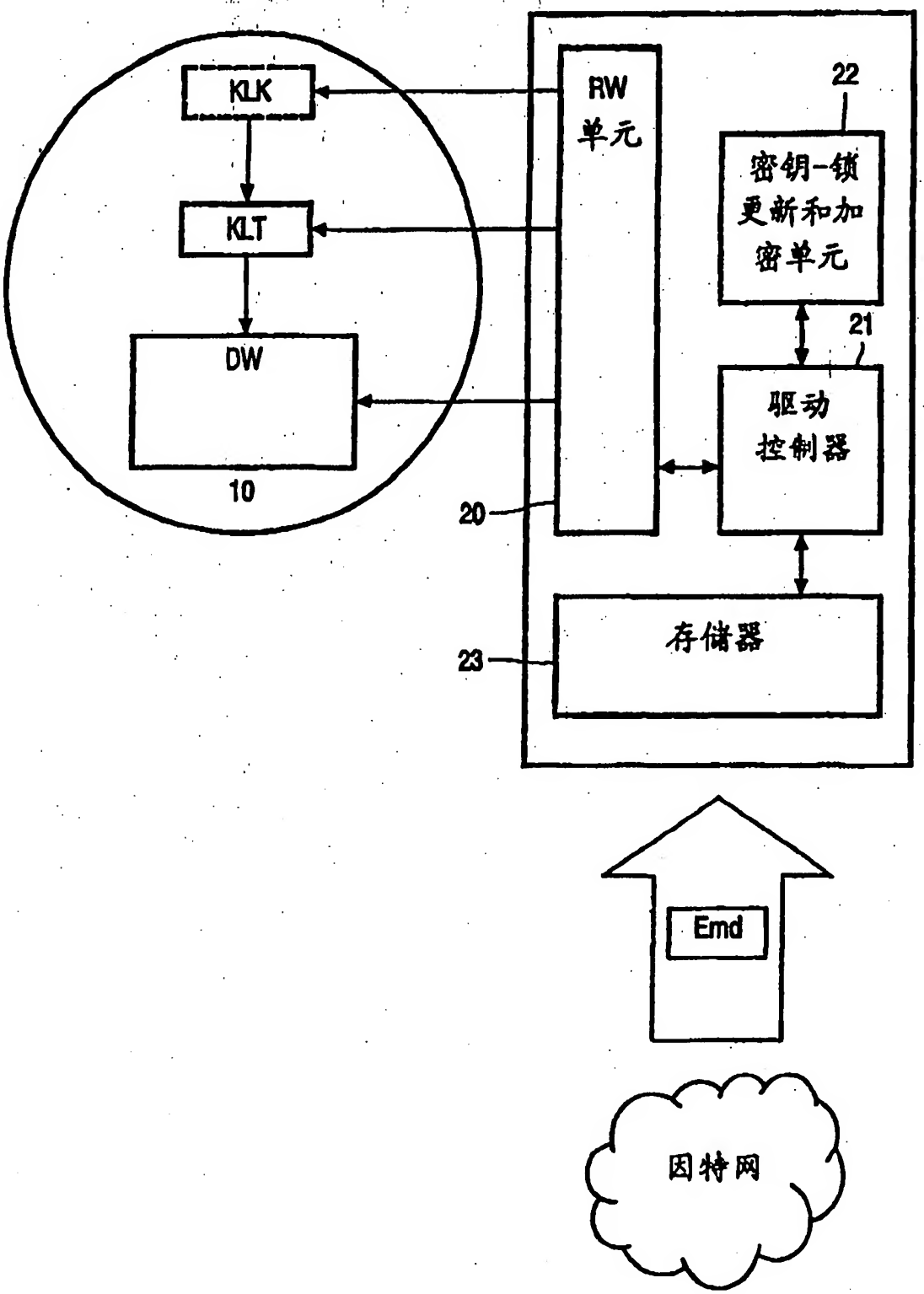


图 2

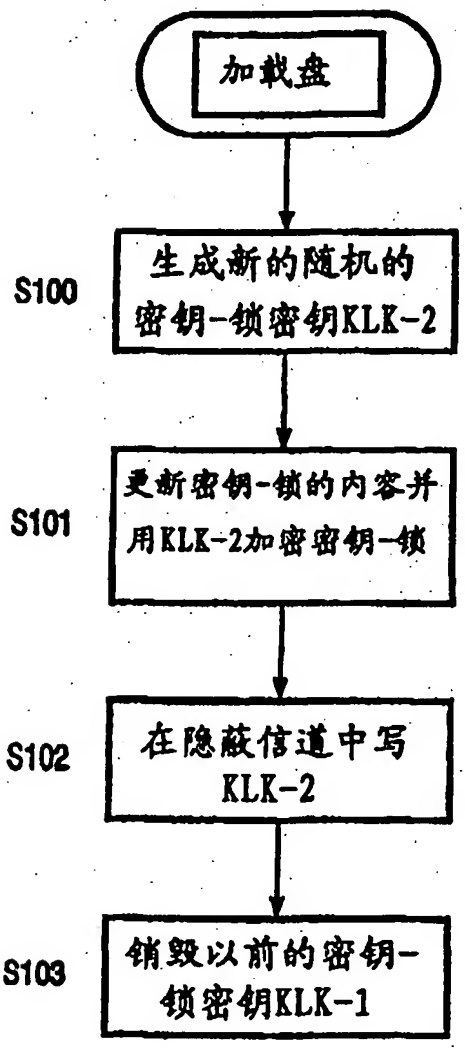

加载盘
S100
生成新的随机的密钥-锁密钥KLK-2
S101
更新密钥-锁的内容并用KLK-2加密密钥-锁
S102
在隐蔽信道中写KLK-2
S103
销毁以前的密钥-锁密钥KLK-1

图 3